وزارة التعليم العالي والبحث العلمي، العراق
جامعة بابل
كلية تكنولوجيا المعلومات
قسم امنية المعلومات
الدراسة: (الصباحية)

تقييم فعالية الشبكات العصبية الإدراكية متعددة الطبقات في أنظمة كشف التسلل

Evaluating the Effectiveness of Multi-Layer Perceptron Neural Networks in Intrusion Detection Systems

مشروع التخرج مقدم كجزء من متطلبات الحصول على درجة البكالوريوس في تخصص امنية المعلومات في تكنولوجيا المعلومات.

A Graduate Project Submitted to the department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfillment of the Requirements for the Bachelor's degree in the Information Security of Information Technology

الطالب

ياسر احمد حسن

بإشراف

م.م. نهى كريم حميد

2023-2024

Abstract

In the rapidly evolving landscape of cybersecurity, Intrusion Detection Systems (IDS) play a pivotal role in safeguarding networks against malicious activities and unauthorized access. With the increasing complexity and diversity of cyber threats, there is a growing demand for advanced detection techniques capable of accurately identifying and mitigating sophisticated intrusions. This project aims to evaluate the effectiveness of Multi-Layer Perceptron (MLP) neural networks as a promising approach for enhancing IDS capabilities.

The proposed research focuses on designing, implementing, and evaluating a tailored MLP neural network architecture specifically optimized for intrusion detection tasks. The project encompasses comprehensive dataset preparation, feature engineering, and model training processes to facilitate robust learning and classification of network traffic patterns associated with normal and malicious activities. Various optimization techniques, including hyperparameter tuning and regularization methods, are employed to enhance the model's performance, scalability, and resilience against overfitting.

A systematic evaluation framework is established to assess the MLP neural network's detection capabilities using a range of performance metrics, such as accuracy, precision, recall, and the area under the Receiver Operating Characteristic (ROC) curve. Comparative analysis with existing intrusion detection methods, including Support Vector Machines (SVM), Random Forest, and Convolutional Neural Networks (CNN), is conducted to benchmark the MLP neural network's performance and identify its strengths and weaknesses in differentiating between benign and malicious network traffic.